UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,379	04/09/2004	Fred Alan Bishop	37355-239	1600

7590 07/26/2007

Gilberto Hernandez
McDermott, Will & Emery
227 West Monroe
Chicago, IL 60606-5096

EXAMINER	
BAYAT, BRADLEY B	
ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/821,379	BISHOP ET AL.	
	Examiner	Art Unit	
	Bradley B. Bayat	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *5, 7-12 and 43-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *5,7-12 and 43-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

As per the amendment submitted on May 1, 2007, claims 5, 43 and 44 have been amended. Thus, claims 5, 7-12 and 43-50 remain pending.

Response to Arguments

Applicant's arguments with respect to the amended claims have been considered but they are not persuasive.

Applicant has amended the claims to include that the scanning is done to a "trusted portion" and contends that differentiates the claim to overcome the outstanding rejection under 103 (response pp. 5-6). However, as disclosed by Foss and illustrated by Figs. 4, rule sets can be established to perform the scanning function according to customization. For instance, if the rule is set to scan a trusted portion as claimed by Applicant, it would be a matter of parameters set out and implemented during the process flow.

Foss discloses in step 408 the system continues scanning the e-mail data packet after having established a rule set. In a preferred embodiment, the scanning function is implemented, in part, by using a searching algorithm. The portions of data processed by the search algorithm are determined according to the protocol. The algorithm may begin processing the data byte by byte and may increase to word by word and to long-word by long-word. The algorithm is typically more efficient if the compare function component in the algorithm can load and compare comparatively large portions of data at a time. Thus, depending on how the data is parsable, the scanning operation may become more efficient as more data is read or once a

particular command or string is detected. The ability to increase the length of data searched and compared depends on the protocol used in transferring the data.

In step 410, the system determines whether the e-mail contains an acceptable or OK command. If the e-mail contains an OK command the system continues with steps following 420 where the e-mail message-data (i.e. the actual message portion of the e-mail) is checked. If the e-mail does not contain an OK command, the system continues with step 412. In step 412, the system translates the unacceptable command to an OK command using the protocol rule set. Different protocols have different rule sets. As mentioned above, the mail guard device can recognize certain protocols. It has rule sets for the protocols it recognizes.

For example, if the e-mail message is sent using SMTP, the device establishes the SMTP rule set which states, among other things, that the acceptable commands are HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. The rule set may also contain certain harmful characters which, if countered, are dropped or translated. Once the rule set has been established in step 406, the scanner knows what to look for. With some protocols, including SMTP, where the data is in ASCII, the search is done byte by byte and does not increase at any point in the processing. For example, with SMTP the search algorithm will search for any of the 128 ASCII characters. If it detects an upper or lower case H, M, R, D, R, N, or Q,--the first letters of the seven acceptable SMTP commands--it will continue scanning. Thus, the scan is done by examining the data one byte at a time.

For example, if it detects a "d", it will continue scanning. If the next byte is any ASCII character other than an "a" (as expected for the DATA command), the scanning will stop and the command will be translated to a NOOP. This function is performed in step 412. If the next byte

is an "a", followed by a "t" and another "a", the scanner knows what is being read is a DATA command and will scan the data that follows accordingly.

Another example using SMTP is the MAIL command. Once the scanner determines that the data scanned is a MAIL command using the same process just described with regard to the DATA command, the scanner will continue scanning for fields it would expect to see after MAIL. Rules of this sort are also contained in the rule set. The first field is the "FROM" field whose data is contained within angled brackets (< and >) and will then look for other fields it would expect to see such as "TO." If the scanner does not find a required field or finds an unacceptable field, it will go to the beginning of the data stream and translate the lead command, in this example the MAIL command, to NOOP and insert blanks or filler after the command and continue. This is done in step 414.

The scanner will also search for certain characters or symbols, such as "?" ".vertline." "<>" and ";" in SMTP, that must be located at particular points in the data for the commands to be processed correctly. Correct usage of these characters are also contained in the rule set. These symbols may indicate the beginning or end of data or have a special role in command syntax. In some cases, if the symbols are out of place or used incorrectly, they can be used to make the mail server perform unauthorized functions. If they are detected and are not in an acceptable sequence, the initial command is translated to a NOOP.

In step 416 the filler data is transmitted to the mail server. At this stage the command and data being sent to the server is harmless to the server and the network. The server will then send an end-of-data response back to the device telling the device that it can now send the next data packet. Each protocol has its own end-of-data response. In SMTP it is the string "250".

The system will continue passing data until it receives an end-of-data indicator. In step 418, the system checks if there are more data packets and, if so, returns to step 400 to determine the port address of the packet.

In step 420 the system continues scanning the e-mail packet. It will do this after determining in step 410 that the e-mail contains an OK command. In step 422 the system determines whether the remaining portion of the e-mail packet contains message-data. Message-data is typically the text portion of the e-mail packet, that is, the actual message being sent from the sender to the receiver. For example, in SMTP, message-data would follow the DATA command. The message-data can be in one of various formats. In a preferred embodiment, the system determines whether the message-data is in ASCII format in step 424. If the message-data is not in ASCII format, the system will discontinue scanning and end the operation. If the message-data is in ASCII format, the system will continue the data scan as shown in step 426.

In step 428 of FIG. 4B, the system checks whether the remaining portion of the e-mail contains acceptable data If the system determines that the data does not contain acceptable characters or symbols, control transfers to step 438 where the system determines whether the data can be made acceptable through translation. If the data is acceptable, the system will continue scanning until it detects a carriage return/line feed (CR/LF) followed by a period (.), followed by another CR/LF. In a preferred embodiment, this sequence of characters and control characters, essentially a period on a line by itself, is an indication that the message-data has ended. In step 432 the system stops scanning and transmits the data to the mail server in step 434. The system will also wait for an end-of-data response from the mail server in step 434. In a preferred embodiment, the end-of-data response is the character string "250". In step 436, the

system will check to see whether there are more data packets and, if so, transfers control to step 400. If there are no more data packets, the process ends and the system waits for the next e-mail connection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5, 7-12 and 43-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guheen et al. (hereinafter Guheen), US 6,473,794 B1 in view of Foss et al. (hereinafter Foss), US 6,298,444 B1.

Claims 5-12

5. Guheen discloses a method for protecting a network server from being used as the basis of an attack on a network client, the method comprising (column 43, lines 34-67; column 248, lines 38-45) and restricting access to said network server to a portion of said network server for at least a selected protocol (column 17, directory services; column 276, line 34-277, line 24). Guheen does not explicitly disclose scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol and removing said particular characters such that a security risk posed by said selected protocol is reduced.

Foss, however, discloses a data scanning network security system wherein portions of a network server are scanned for particular characters, said particular characters being associated

with said selected protocol and removing said particular characters such that a security risk posed by said selected protocol is reduced (column 4, lines 5-50, column 5, lines 3-11 and lines 39-45, column 6, lines 20-25, column 7, lines 1-3, 48-59). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Guheen's network security system to include scanning a trusted portion of electronic data transfer to a server to ensure that harmful or unwanted characters do not enter a network, as per teaching of Foss (column 1, line 8-column 2, line 39).

7. The method of claim 5, further comprising replacing said particular characters with benign characters such that a security risk posed by said selected protocol is reduced (column 272, line 30-column 259, line 30).

8. The method of claim 5, wherein said characters are hostile characters and wherein if a request contains any of said hostile characters, the request is rejected (column 273, lines 16-34; column 280, lines 19-39).

9. The method of claim 5, further comprising logging said particular characters to form a security log (column 266, lines 12-21, column 268, lines 20-36, column 286, lines 13-58).

10. The method of claim 9, further comprising reviewing said security log to determine whether said particular characters are hostile (column 43, line 34-column 44, line 8).

11. The method of claim 5, wherein said protection of the network server is accomplished during an electronic purchase transaction (column 251, lines 34-36).

12. The method of claim 11, wherein the electronic purchase transaction is conducted using a digital wallet (column 17, java wallet; column 261, lines 30-53).

Claims 43-50

43. Guheen discloses a computer-implemented method for protecting a network server from being used as the basis of an attack on a network client, the method comprising: a. receiving a request for a connection at said server from said network client (figure 87, 2613; receiving user indicia); d. verifying that any response from said network server to said network client is void of said particular characters (fig 88, 2700; allowing browser-based authentication with user verification data); and e. providing said response from said network server to said network client (fig 88, 2702; granting access to at least one of application and system data based on the user verification data).

Guheen does not explicitly disclose scanning said portion of said network server for particular characters, said particular characters being associated with said selected protocol and removing said particular characters such that a security risk posed by said selected protocol is reduced.

Foss, however, discloses a data scanning network security system wherein portions of a network server are scanned for particular characters, said particular characters being associated with said selected protocol and removing said particular characters such that a security risk posed

by said selected protocol is reduced (column 4, lines 5-50, column 5, lines 3-11 and lines 39-45, column 6, lines 20-25, column 7, lines 1-3, 48-59). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Guheen's network security system to include scanning of electronic data transfer to a server to ensure that harmful or unwanted characters do not enter a network, as per teaching of Foss (column 1, line 8-column 2, line 39).

44. The method of claim 43 further comprising restricting access to said network server for said protocol to said portion of said network server (column 17, directory services; column 276, line 34-277, line 24).

45. The method of claim 43 further comprising replacing said particular characters with benign characters such that a security risk posed by said selected protocol is reduced (column 272, line 30-column 259, line 30).

46. The method of claim 43 wherein said protocol comprises JavaScript (column 34, lines 10-60).

47. The method of claim 43 further comprising logging said particular characters to form a security log (column 266, lines 12-21, column 268, lines 20-36, column 286, lines 13-58).

48. The method of claim 47 further comprising reviewing said security log to determine whether

said particular characters are hostile (column 273, lines 16-34; column 280, lines 19-39).

49. The method of claim 47 wherein said protection of the network server is accomplished during an electronic purchase transaction (column 251, lines 34-36).

50. The method of claim 49 wherein the electronic purchase transaction is conducted using a digital wallet (column 17, java wallet, column 261, lines 30-53).

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday-Friday 8 a.m.-6:30 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on 571-272-6779. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Bradley B. Bayat
Primary Examiner
Art Unit 3621